FOR INFORMATION

EBAP/18/50

June 4, 2018

To: Members of the Executive Board

From: The Secretary

Subject: **Office of Internal Audit—FY 2018 Activity Report**

Board Action:	Executive Directors' **information**
Publication:	No, due to content sensitivity.
Additional Information:	Ahead of the visit of the External Audit Committee, OIA will be available in the Board Committee room on June 12, 2018 to answer questions on this Activity Report.
Questions:	Ms. Onyango, OIA (ext. 30511) Mr. Murugan, OIA (ext. 38132)

INTERNATIONAL MONETARY FUND

June 1, 2018

OFFICE OF INTERNAL AUDIT (OIA)
FY 2018 ACTIVITY REPORT

EXECUTIVE SUMMARY

This report provides an overview of OIA's activities for the full year of FY 2018, and builds on the interim activity report issued in January 2018. The report fulfills management's commitment to keep the Executive Board regularly informed on audit and control-related items.

FY 2018 marked the first year where OIA's outputs spanned all its reporting formats, including the two new approaches to reporting (Insight Notes and Good Practice Series) introduced during the year. OIA finalized three audit and advisory reports during FY 2018 covering: (i) the audit of third party vendor management; (ii) the audit of systems development and maintenance processes; and (iii) the advisory review of the results-based management for capacity development. OIA is also in the process of finalizing recommendations for two ongoing advisory reviews relating to (i) talent acquisition and the (ii) committee structure for risk management. OIA completed its first "Insight Note" covering the Fund's approach to issuing, updating, and enforcing its administrative policies. As part of its "Good Practice Series" offerings, OIA covered topics of: (i) the "Three Lines of Defense" model; (ii) Ransomware; and (iii) the General Data Protection Regulation and Data Privacy.

OIA also issued the Ninth Periodic Monitoring Report during the year. The report assesses the extent to which Board-endorsed IEO recommendations have either been implemented or are in progress. The Evaluation Committee (EVC) of the Board is scheduled to discuss the PMR on June 19, 2018.

OIA formulated its Program of Work for FY19, comprising a balanced mix of audit coverage and advisory reviews. The Program of Work is designed to support the operationalization of key initiatives, while also providing assurance on foundational, mature business processes. A new "delivery" model, better leveraging OIA staff's competencies, will be implemented to execute the ambitious Program of Work for FY19.

An External Quality Assessment (EQA) of OIA was conducted in April 2018. OIA received a "generally conforms" rating, which is the highest available rating in the assessment. Opportunities for continuous improvement were also flagged, and action plans have been formulated to address the gaps.

Approved By
Nancy Onyango

Prepared by Office of Internal Audit

CONTENTS

INTRODUCTION

1. This report fulfills the Managing Director's commitment to regularly share information with the Board on audit and control-related matters, and provides an overview of the Office of Internal Audit's (OIA) activities in FY 2018.

2. On June 12, 2018, a question and answer (Q&A) session with OIA is scheduled for Executive Directors and their offices. This session will help Executive Directors to prepare for the visit of the External Audit Committee (EAC) by providing an opportunity to discuss the results of FY 2018 work with the OIA team.

OIA'S MANDATE

3. OIA is an independent assurance and advisory function designed to protect and strengthen the Fund. The mission of OIA is to: (i) bring a systematic and disciplined approach to assess and improve the effectiveness of the Fund's governance, risk management processes, and internal controls; and (ii) act as an advisor and catalyst for the improvement of the Fund's business processes by advising on best practice and the development of cost-effective control solutions.

4. OIA's work is carried out in accordance with the Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF). To provide for the independence of OIA, the Director of OIA reports to Fund management, and maintains a functional reporting relationship with the EAC.

SUMMARY OF WORK COMPLETED IN FY 2018

A. Insight Note on Fund's Administrative Policies and Procedures (issued July 2017)

5. OIA's first "Insight Note" - a new reporting format designed to contribute to institutional problem-solving – covered the Fund's approach to issuing, documenting, updating, and enforcing administrative policies. The Insight Note, produced with the support of LEG, identified areas of weaknesses in the Fund's handling of administrative policy, procedures, and guidance, and suggested certain improvements for management's consideration. The systemic weaknesses identified covered: (i) hierarchy and level of authority underpinning Fund administrative policies and procedures (including delineating between mandatory policy and optional guidance); (ii) documentation, communication, and access; and (iii) accountability, ownership, and enforcement.

6. LEG, working with relevant departments, launched the new Administrative Manual in April 2018, bringing together non-employment administrative rules in one place, online. The next phase of LEG's efforts, will focus on establishing a document hierarchy (to better delineate between mandatory policy and optional guidance) and promulgating a Fund-wide "Policy on

Policies", to define, standardize and streamline the processes for issuing, monitoring and updating administrative policies.

B. Audit of Third Party Vendor Management (issued September 2017)

7. The audit assessed the robustness of the Fund's approach to managing risks associated with third party vendors throughout the lifecycle of the vendors' engagement with the Fund. The audit concluded that there are foundational weaknesses in the Fund's approach to managing third party risks after contracts have been awarded. Specifically: (i) there are no clearly defined governance arrangements in place; (ii) weaknesses exist in the risk assessment methodology used to assess and prioritize vendor-related risks for monitoring; (iii) there are limitations in the coverage and design of current monitoring processes; and, (iv) the Fund's ability to holistically analyze third party risk information and performance is limited.

8. CSF is pursuing a sound approach for remediation of the identified issues, and is working on establishing a holistic third-party risk management framework that is suitably informed by the Fund's risk acceptance and resource availability. Once this overarching framework is established, the subsequent implementation efforts will be suitably guided by the principles set out in the framework.

C. Good Practice Series (GPS) on the Three Lines of Defense (3LOD) Model (issued October 2017)

9. With a view to supporting the institutional goal of integrating risk management into the Fund's operational fabric, OIA published the first edition of its "Good Practice Series" (GPS) – covering the "Three Lines of Defense" (3LOD) model. The model is a well-established governance framework for risk management (used by global and domestic regulators) that is predicated on defining clear roles and responsibilities, and on maintaining separation of roles among the various groups involved in risk management.

10. The GPS provided an overview of the distinct roles played by the three "lines" within the Fund's governance framework, with the Board and Management being the primary stakeholders served by the lines. The GPS also outlined the benefits of the model, its key foundational elements, efforts underway within the Fund to promote greater risk accountability, and some key indicators for assessing effective operationalization of the model.

D. Audit of the Fund Systems Development and Maintenance Processes (issued November 2017)

11. The audit assessed the design and effectiveness of the Fund's SDLC processes for managing risks that impact the overall quality of the software solution, the total cost of delivery, and the security of the Fund's information.

12. The audit noted the lack of clearly articulated risk-based requirements for SDLC activities at the institutional level, resulting in significant weaknesses in the Fund's software development approach. The audit results emphasized the need for urgent attention in mandating and enforcing improved SDLC controls across the Fund. ITD provided a combination of near-term and medium-term measures to address the issues highlighted in this report.

E. Advisory Review of the Results Based Management (RBM) Initiative for Capacity Development (issued March 2018)

13. The operationalization of Results-Based Management (RBM) is an integral component of the broader Capacity Development (CD) reform effort in the Fund. The implementation of RBM is intended to help the Fund: (i) monitor and evaluate the successes and failures of CD more effectively; and (ii) set priorities for resource allocation by firmly focusing CD on results.

14. The objective of OIA's advisory was to draw lessons from the RBM implementation efforts to date and provide a forward-looking perspective to inform the trajectory of work on RBM and the broader CD business process and system reform.

15. The ongoing implementation efforts have yielded some notable gains - the development of a Fund-wide catalog of standardized objectives and indicators, a consolidated institutional inventory of CD projects, the design of initial standardized reports and dashboards, and the training of many staff. It will be important to preserve and build on these gains going forward. The advisory review also highlighted areas for improvement, including the need to: (i) better estimate the change management effort and consider dependencies on broader CD business process changes; (ii) have a robust and well-resourced program governance framework for timely decision-making; and (iii) adopt a flexible technology platform to meet the rather bespoke nature of Fund CD processes and facilitate broad-based user adoption. Time-bound action plans have been designed (and are currently being implemented) to address the highlighted issues.

F. Good Practice Series (GPS) on Ransomware (issued March 2018)

16. OIA's second edition of its GPS product offering covered the topical subject of Ransomware. Ransomware is a malicious computer program that restricts access to data by encrypting files or locking computer screens, allowing attackers to hold computer files "hostage" and attempt to extort money by asking for "ransom." It exploits security vulnerabilities in technology systems.

17. Many of the Fund's existing information security controls contribute towards managing the risk of ransomware attacks. For the most part, ransomware protection is and should be embedded within the Fund's broader efforts to maintain overall information security hygiene and business continuity. Articulating the Fund's overall position for handling ransomware events, simulating scenarios of ransomware attacks, routinely assessing the Fund's defenses, and

continuing to heighten end-user awareness will be important preventative considerations in addressing ransomware attacks.

G. Good Practice Series (GPS) on General Data Protection Regulation (finalized and issued in May 2018)

18. OIA's third and most recent edition of its GPS series was initiated in FY 2018 (finalized and issued in May 2018) and provided an overview of the new "EU General Data Protection Regulation" (GDPR) and privacy protection at the Fund. The GPS provides a primer on the key requirements of GDPR, and more importantly, highlights data privacy mechanisms in the Fund, in the context of an increasingly digital and networked world, where organizational strategies and decisions are often informed by insights obtained from the analysis of vast volumes of data, including personal data. This emerging landscape is also increasingly characterized by misuse or breaches of personal data.

19. The GPS posits that the GDPR (which went into effect on 25th May, 2018) could be indicative of an emerging shift in posture for data privacy regulation around the world. Although the GDPR may not be directly binding on the Fund, the introduction of the GDPR could potentially pose reputational or operational risks to the Fund if baseline privacy measures are not in place. Given the strict accountability that the GDPR introduces, impacted third-parties from whom the Fund collects personal data may particularly want to ensure that the Fund has an "adequate level of protection" over such data. The introduction of the GDPR provides the Fund an opportunity to reassess its privacy controls and effectively embed personal data protection into its processes. Designing a realistic plan can offer the Fund a defensible and cost-effective approach to data privacy while also taking into account consideration leading data privacy practices. In this context, the GPS outlines some key considerations, going forward, to support the ongoing institutional deliberations on GDPR and data privacy.

SUMMARY OF WORK UNDERWAY IN FY 2018

A. Advisory Review of Talent Acquisition (reporting underway)

20. The ability to attract and retain the best talent for the Fund's evolving priorities is central to the institution's AIM agenda. At the request of HRD management, this advisory review supports the planned redesign of the Fund's talent acquisition program in the context of the HR strategy and the modernization of HR processes and technology (1HR).

21. The objective of this advisory engagement is to review the effectiveness and efficiency of the Fund's talent acquisition program in meeting the Fund's needs, and provide forward-looking recommendations based on leading practices. The review's preliminary findings are geared towards supporting HRD's vision of repositioning the talent acquisition process as a more strategic activity – one that goes beyond routine and reactive vacancy filling to a more pro-active,

value-driven model that enables talent forecasting and promotes hiring manager collaboration through appropriate assessment tools, incentives, and accountability mechanisms. OIA's review indicates that, to realize this broader goal, additional work is needed - in strengthening governance and oversight, leveraging the supporting technology for greater efficiencies and consistency in work practices, and investing in the development of insightful people analytics.

22. As a separate output, this advisory review of talent acquisition also focuses on field-based short-term experts. The heavily decentralized nature of the appointments of field-based short-term experts warranted a separate assessment of the risks and reporting of the results. This "carve-out" piece of work (from the broader talent acquisition advisory review) focuses on the governance, oversight, and working practices for the engagement of field-based short-term experts. Preliminary findings of the review suggest that improvements are needed in: governance and oversight, including policies and accountabilities; consistency of hiring practices (sourcing, screening, and compliance with policies for nepotism and conflicts of interest); transparency in the assignment and use of experts; rate-setting and compensation; and management information and technology support. The report will be finalized in June 2018.

B. Advisory Review of the Committee Structure for Risk Management (reporting underway)

23. A key priority for the Fund Risk Committee (FRC) and the Office of Risk Management (ORM) is to foster a stronger risk culture within the organization and facilitate further integration of risk management into the Fund's operational fabric. With the establishment of the FRC, it will be important to clarify the roles and responsibilities of the various standing committees across the Fund (such as the Security Policy Group, Committee on Business and Information Technology) including vis-à-vis the FRC – to facilitate systematic, coordinated, and holistic risk oversight.

24. This OIA advisory engagement is designed to support the efforts of the FRC and ORM by providing tailored recommendations to enhance the robustness of the overall risk architecture. As part of this advisory review, OIA has compiled a detailed inventory of the various governance bodies within the Fund that have some degree of risk management or risk oversight responsibilities, documenting their roles, responsibilities, coverage and decision authority. The OIA inventory is designed to inform a more holistic view of the completeness and adequacy of risk coverage from an institutional perspective.

25. Preliminary findings suggest the need for a more granular codification of the remit and responsibilities of the FRC. Additional recommendations are also being formulated to streamline the Committee structures to enable a sharper institutional focus on risk management and risk mitigation. The report is expected to be finalized in June 2018.

NINTH PERIODIC MONITORING REPORT

26. OIA has completed the Ninth Periodic Monitoring Report (PMR) on the Status of Management Implementation Plans (MIPs) in Response to Board-Endorsed Independent Evaluation Office (IEO) Recommendations. The report assessed the progress made over the last year on actions contained in two "new" MIPs arising from recent IEO evaluations, and another seven for which individual management actions were classified as "open" in the Eighth PMR. . The report highlighted the positive traction on the last four MIPs, but also indicated that older actions appear challenging to implement. Actions that are not implemented within the first few years, after a MIP is approved, tend to be more difficult or intractable. The report is expected to be discussed at the Evaluation Committee (EVC) of the Board on June 19, 2018.

27. Building on the improvements in the previous year, the PMR introduced several novel ideas to assist management and the Board with a clearer view of where management or Board intervention may be required. At the request of the EVC, OIA also performed an analysis of open management actions and made suggestions on possible approaches for addressing the long-standing actions. This analysis serves as an input to ongoing deliberations by the EVC and the external evaluation of the IEO.

28. Earlier in the year, OIA also published an online repository of the population of IEO recommendations and related management actions. The repository, which is hosted on OIA's website, is intended to provide Executive Directors and staff with a full view of the population of past IEO recommendations and their eventual disposition.

OVERDUE AUDIT ISSUES

29. OIA issued its six-monthly "snapshot" report on overdue audit issues as of April 30, 2018 (see Appendix I). The report noted that timely mitigation of identified control gaps remains a challenge, particularly where the issues are of a strategic nature and the risks are shared across multiple departments. OIA will continue to foster a more "risk-aware" culture within the organization by heightening sensitivity on overdue issues and by reinforcing ownership of risk mitigation actions.

PROGRAM OF WORK FOR FY19

30. OIA formulated its Program of Work for FY19, building on prior years' efforts to take on a more strategically-relevant role in the Fund. The Program of Work is guided by three over-arching goals: (i) deliver value-added results that are aligned with institutional focus areas, priority risk themes, and stakeholder needs; (ii) provide assurance on foundational and mature business processes within the Fund; and (iii) play a catalytic role in improving the Fund's business processes. In pursuing these goals, OIA is looking to build on the gains derived through its "collaborative model" of partnering closely with client departments, by offering a proactive perspective on significant risks, providing timely insights on key strategic initiatives, and fostering a more risk and

controls-focused culture within the organization. In addition to the proposed pipeline for FY19, the Program of Work provides stakeholders with greater visibility into a longer-term view of potential OIA coverage areas over FY20-21.

31. The FY19 program of work comprises a balanced mix of audit coverage and advisory reviews: (i) to support the operationalization of key institutional initiatives - 1HR, people analytics (as part of HR strategy), and the institutional program and change management infrastructure; and (ii) to provide assurance on foundational business processes - such as quality assurance for TA delivery, IT managed services, Fund's overseas presence, payment and SWIFT infrastructure, third-party administered insurance programs, network security, and pension fund administration. In addition, the program of work will also seek to mainstream the roll-out of OIA's new reporting formats - Insight Notes and the Good Practice Series (GPS).

FY19 ENGAGEMENTS – SUMMARY OF WORK INITIATED

A. Advisory Review of the Fund's Compliance Activities (fieldwork underway)

32. A compliance program is a formal system of activities that aims to help an organization promote adherence to its legal, contractual, and ethical obligations, and uphold internal policies, procedures, standards and codes of conduct. Formal compliance programs have grown in importance, especially in regulated organizations. Compliance requirements at the Fund may be driven by a voluntary adherence to external regulations, commitments to agreements, or internally established policies and standards.

33. The objective of OIA's advisory review is to inform the ongoing deliberation on the Fund's approach for covering broader compliance risks, and to support ORM's efforts to formulate a view from a risk management perspective regarding the Fund's existing compliance activities.

B. Insight Note on Project and Change Management (fieldwork underway)

34. OIA's second Insight Note, designed to contribute to institutional problem-solving by leveraging OIA's understanding of the organization's risk management and governance processes, supports ongoing efforts at strengthening project and change management. The Fund is increasingly undertaking multi-million-dollar programs that extend beyond single IT implementation projects, and involve significant changes to processes and practices. These projects, which have increased lately in line with the drive to modernize work practices, straddle both core and cross-functional areas of the Fund. The Insight Note would propose a tailored approach for program and change management that strikes the right balance between applicable standards, frameworks and leading practices and the needs of an organization with infrequent large projects.

C. Review of the Fund's Overseas Presence (engagement approach adjusted, planning underway)

35. The Fund's overseas footprint is an important part of the member engagement strategy. The Fund's primary business model for engaging members is to travel from HQ to conduct surveillance activities, negotiate Fund-supported programs, and deliver capacity development (CD). This model is supplemented by resident representatives and regional offices in selected countries, and technical assistance and training centers to bring the delivery of CD closer to the users.

36. While originally anticipated as an advisory engagement, after considering feedback from initial stakeholder consultations, OIA has decided to adopt a phased approach in performing this engagement. As an initial phase, OIA will perform an audit to holistically assess the design of the control framework and administrative arrangements in place for supporting the Fund's overseas presence. The audit would focus on governance provisions, clarity of roles and responsibilities, accountabilities, and control mechanisms to ensure effective oversight and compliance. Based on the outcomes of this audit, OIA may evaluate performing subsequent "deep-dives" on specific aspects relating to overseas presence, in an audit or advisory capacity.

EXTERNAL QUALITY ASSESSMENT

37. OIA underwent an External Quality Assessment (EQA) in April 2018. The International Standards for the Professional Practice of Internal Auditing ("Standards") stipulate that "External Assessments must be conducted at least every five years by a qualified, independent assessor or assessment team from outside the organization". The principal objectives of the EQA, which were led by the Institute of Internal Auditors (IIA), were to assess OIA's conformance with the Standards and identify opportunities for continuous improvement in OIA's performance.

38. OIA received the highest rating (of "generally conforms") in the assessment. This rating denotes that the relevant structures, policies, and procedures of OIA's activities, as well as the processes by which they are applied, comply with the requirements of the Standards and the IIA Code of Ethics in all material respects. The external assessment also identified gaps and opportunities for continuous improvement. The primary recommendations related to: (i) finalizing the documentation of specific components of OIA's internal audit methodology and processes; (ii) more consistently communicating the results of OIA's revamped Quality Assurance and Improvement (QAIP) program to stakeholders; and (iii) continuing to closely monitor and document the resourcing needs to execute OIA's risk-based Program of Work. OIA has formulated a comprehensive action plan to address these gaps, most of which are defined for implementation by end of FY19.

STAFFING & BUDGET

39. Under the leadership of OIA's new Director, the OIA Management team will focus on providing "richer" job assignments that are tailored to leverage staff's competencies. Changes in the "delivery model" will also be implemented in FY19 to afford greater opportunities for senior staff to demonstrate their technical and leadership competencies. The proposed delivery model is also intended to increase the overall productivity of the function.

40. OIA used 99 percent of its overall budget of $5.0 million in FY 2018.

Appendix I. Report on Overdue Audit Issues as at April 30, 2018

Key Messages

This report presents an overview of outstanding and overdue audit issues. Since the issuance of the last report, OIA closed only one issue to bring the number of outstanding issues to 30 as of April 30, 2018. Of the total outstanding, 16 are overdue, a relatively high percentage. Half of the overdue issues are rated as "High" impact. Timely remediation of control gaps remains a challenge and this is especially true where the issues are of a cross-cutting nature and implementation efforts straddle multiple departments that often have competing priorities.

- ITD has been making progress towards implementing the near-term actions (originally due on January 31, 2018) to address OIA's Audit of the Fund's **Systems Development and Maintenance Processes,** including prioritizing some actions, e.g. production access and accounts. It will be particularly important to establish the policy posture, scope, and roles and responsibilities relating to "business-led" software development and maintenance activities in a timely manner.
- Efforts are underway by CSF to propose enhancements to the Fund's **Third Party Vendor Risk Management** framework (originally due on January 31, 2018) and **Business Continuity Management** strategy (originally due on March 31, 2018) to address issues identified by OIA's audits. Comprehensive proposals are currently being drafted for management's consideration.
- ITD is working to enhance the Fund's governance model for **Identity and Access Management** with the help of external subject matter experts. After some initial delay in sourcing external expertise, a project plan has been designed and implementation efforts (including department stakeholder engagement) are currently underway (originally due on April 30, 2018). Progress has also been made in inventorying privileged (super user) accounts. A well-defined IAM governance model is a key enabler for the Fund's ongoing system implementation and cloud migration efforts. Notwithstanding the competing work program demands on ITD, it will be important to steadily support the implementation of this action plan in a timely manner.
- The High impact issue on the development of a holistic control framework (originally due on April 30, 2015) to support **the administration of salaries and benefits** remains significantly overdue. Following recent efforts to bring this action back on track, HRD is continuing its phased approach with: (i) business process re-design in preparation of the new HR solution (1HR) which entails streamlining current processes and interactive learning sessions to facilitate internal control conversations; and (ii) upon selecting a solution, process level control design and implementation. Therefore, substantial implementation of the control framework is unlikely before the first phase of technology deployment in early 2020.

With regard to issues rated as "Medium" impact:

- ITD has designed a set of comprehensive plans to strengthen the Fund's **software license management.** While efforts are underway, there have been slippages (up to five quarters in some cases) in implementing these plans. Greater focus on project execution will be key to avoid further slippages.
- A long-standing action item on **Database Monitoring** has been completed; ITD has designed a risk-based plan for identifying, prioritizing and monitoring Fund databases.

Figure 1. Overdue Audit Issues (past due date)

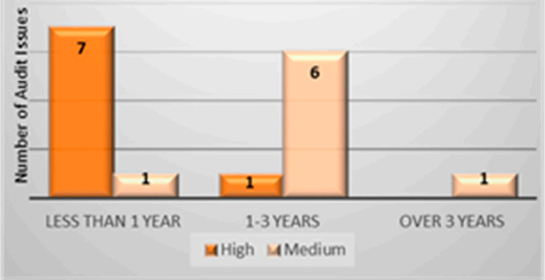
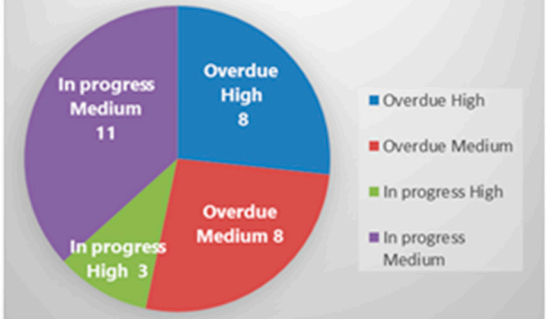


Figure 2. Outstanding Audit Issues



International Standards for the Professional Practice of Internal Auditing

2500 – Monitoring Progress: The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 - The chief audit executive must ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.